03-16-00

A

Please type a plus sign (+) inside this box [+]

PTO/SB/05 (12/97)
Approved for use through 09/30/00. OMB 0651-0032
Patent and Trademark Office: U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

UTILITY PATENT APPLICATION TRANSMITTAL

(Only for new nonprovisional applications under 37 CFR 1.53(b)

Attorney Docket No. 042390.P7440 Total Pages 3

First Named Inventor or Application Identifier Mittal, Millind et al.

Express Mail Label No. EL431890705US

ADDRESS TO: **Assistant Commissioner for Patents**
Box Patent Application
Washington, D. C. 20231

APPLICATION ELEMENTS
See MPEP chapter 600 concerning utility patent application contents.

1. XX Fee Transmittal Form
(Submit an original, and a duplicate for fee processing)

2. XX Specification (Total Pages 19)
(preferred arrangement set forth below)
- Descriptive Title of the Invention
- Cross References to Related Applications
- Statement Regarding Fed sponsored R & D
- Reference to Microfiche Appendix
- Background of the Invention
- Brief Summary of the Invention
- Brief Description of the Drawings (if filed)
- Detailed Description
- Claims
- Abstract of the Disclosure

3. XX Drawings(s) (35 USC 113) (Total Sheets 3)

4. XX Oath or Declaration (Total Pages 4)
a. XX Newly Executed (Original or Copy)
b. ____ Copy from a Prior Application (37 CFR 1.63(d))
(for Continuation/Divisional with Box 17 completed) **(Note Box 5 below)**
i. ____ DELETIONS OF INVENTOR(S) Signed statement attached deleting inventor(s) named in the prior application, see 37 CFR 1.63(d)(2) and 1.33(b).

5. ____ Incorporation By Reference (useable if Box 4b is checked)
The entire disclosure of the prior application, from which a copy of the oath or declaration is supplied under Box 4b, is considered as being part of the disclosure of the accompanying application and is hereby incorporated by reference therein.

6. ____ Microfiche Computer Program (Appendix)

7. ____ Nucleotide and/or Amino Acid Sequence Submission
(if applicable, all necessary)
a. ____ Computer Readable Copy
b. ____ Paper Copy (identical to computer copy)
c. ____ Statement verifying identity of above copies

ACCOMPANYING APPLICATION PARTS

8. XX Assignment Papers (cover sheet & documents(s))

9. XX a. 37 CFR 3.73(b) Statement (where there is an assignee)

XX b. Power of Attorney

10. ____ English Translation Document (if applicable)

11. ____ a. Information Disclosure Statement (IDS)/PTO-1449

____ b. Copies of IDS Citations

12. ____ Preliminary Amendment

13. XX Return Receipt Postcard (MPEP 503) (Should be specifically itemized)

14. ____ a. Small Entity Statement(s)

b. Statement filed in prior application, Status still proper and desired

15. ____ Certified Copy of Priority Document(s) (if foreign priority is claimed)

16. XX Other: Certificate of Express Mail with copy of postcard showing contents of Express mail package.

17. **If a CONTINUING APPLICATION,** check appropriate box and supply the requisite information:

___ Continuation ____ Divisional ____ Continuation-in-part (CIP)

of prior application No: ____________________

18. **Correspondence Address**

____ Customer Number or Bar Code Label ____________________
(Insert Customer No. or Attach Bar Code Label here)

or

X Correspondence Address Below

NAME Michael A. Bernadicou
BLAKELY, SOKOLOFF, TAYLOR & ZAFMAN LLP

ADDRESS 12400 Wilshire Boulevard
Seventh Floor

CITY Los Angeles STATE California ZIP CODE 90025-1026

Country U.S.A. TELEPHONE (408) 720-8300 FAX (408) 720-9397

EXPRESS MAIL CERTIFICATE OF MAILING

"Express Mail" mailing label number: EL431890705US

Date of Deposit: March 14, 2000

I hereby certify that I am causing this paper or fee to be deposited with the United States Postal Service "Express Mail Post Office to Addressee" service on the date indicated above and that this paper or fee has been addressed to the Assistant Commissioner for Patents, Washington, D. C. 20231

Iola Rodriguez

(Typed or printed name of person mailing paper or fee)

I Rodriguez

(Signature of person mailing paper or fee)

3/14/00

(Date signed)

Serial/Patent No.: Not yet assigned Filing/Issue Date: Herewith

Client: INTEL CORPORATION

Title: METHOL AND APPARATUS FOR HARDWARE PLATFORM INDENTIFICATION WITH PRIVACY PROTECTION

BSTZ File No.: 042390.P7440 Atty/Secty Initials: MAB/MVS/1r

Date Mailed: 3/14/00 Docket Due Date: * * *

The following has been received in the U.S. Patent & Trademark Office on the date stamped hereon:

- □ Amendment/Response (_____ pgs.)
- □ Appeal Brief (_____ pgs.) (in triplicate)
- ■ Application - Utility (19 pgs., with cover and abstract)
- □ Application - Rule 1.53(b) Continuation (_____ pgs.)
- □ Application - Rule 1.53(b) Divisional (_____ pgs.)
- □ Application - Rule 1.53(b) CIP (_____ pgs.)
- □ Application - Rule 1.53(d) CPA Transmittal (_____ pgs.)
- □ Application - Design (_____ pgs.)
- □ Application - PCT (_____ pgs.)
- □ Application - Provisional (_____ pgs.)
- ■ Assignment and Cover Sheet
- ■ Certificate of Mailing
- ■ Declaration & POA (8 pgs.)
- □ Disclosure Docs & Orig & Copy of Inventor's Signed Letter (_____ pgs)
- ■ Drawings: 3 # of sheets includes 5 figures
- ■ Express Mail No. EL431890705US
- □ _________ Month(s) Extension of Time
- □ Information Disclosure Statement & PTO-1449 (__ pgs.)
- □ Issue Fee Transmittal
- □ Notice of Appeal
- □ Petition for Extension of Time
- □ Petition for ____________
- ■ Postcard
- □ Power of Attorney (_____ pgs.)
- □ Preliminary Amendment (_____ pgs.)
- □ Reply Brief (_____ pgs.)
- □ Response to Notice of Missing Parts
- □ Small Entity Declaration for Indep. Inventor/Small Business
- ■ ~~Transmittal Letter, in duplicate~~
- ■ Fee Transmittal, in duplicate
- ■ Check No. 34167 Amt: $1074.00
- ■ Check No. 34131 Amt: $40.00
- ■ 34132 $40.00

□ Other: ____________

EL431890705US

Our Ref.: 42390.P7440

UNITED STATES PATENT APPLICATION

FOR

METHOD AND APPARATUS FOR HARDWARE PLATFORM IDENTIFICATION WITH PRIVACY PROTECTION

Inventors:

Millind Mittal
James Mi

Prepared By:

BLAKELY, SOKOLOFF, TAYLOR & ZAFMAN
12400 Wilshire Blvd., 7th Floor
Los Angeles, California 90025-1026
(310) 207-3800

"Express Mail" mailing label number: EL431890705US
Date of Deposit: March 14, 2000
I hereby certify that I am causing this paper or fee to be deposited with the United States Postal Service "Express Mail Post Office to Addressee" service on the date indicated above and that this paper or fee has been addressed to the Commissioner of Patents and Trademarks, Washington, D.C. 20231

LOLA RODRIGUEZ
(Typed or printed name of person mailing paper or fee)

L Rodriguez
(Signature of person mailing paper or fee)

3/14/00
(Date signed)

METHOD AND APPARATUS FOR HARDWARE PLATFORM IDENTIFICATION WITH PRIVACY PROTECTION

FIELD OF THE INVENTION

The present invention relates to computer system identification. More specifically, the invention relates to a method and apparatus for identifying a computer system, while inhibiting the ability to track user communication with different web sites.

BACKGROUND OF THE INVENTION

A content provider that delivers encrypted content and a decryption program (such as from a web site) to computer systems may want to ensure that only authorized systems may execute that program. By including in the decryption program instructions that enable that program to identify the computer system that executes it, the program can determine whether that system is authorized to run the program. If the program determines that the system is not authorized, it can discontinue execution.

An embedded identifier stored within a computer system, such as a processor serial number (hereinafter described as a “processor number”), may provide an effective way for such a program to identify such a system – if the program can retrieve that identifier, e.g., via a ring 3 instruction. Such an instruction, however, exposes the same identifier each time a system chooses to identify itself. Although this may not be particularly significant when identifying a platform to a decryption program, providing access to such a platform identifier may enable tracking of a user’s Internet activity, which could enable compilation of information that links the user to various web sites.

One way to impede collection of such information is to customize the identifier for each web site. For example, in response to an identification request, a computer system may return a hash value that is a function of a processor number and a key that is unique for each web site. See copending application serial number 09/259,620, filed February 26, 1999 and assigned to this application's assignee. As shown in figure 1, web sites 36a-c may provide unique keys 34a-c, respectively, which encryption unit 31 hashes with processor number 30, producing unique hash values 32a-c for identifying computer system 10 to each web site. As a result, each web site 36a-c may identify system 10 by a different hash value 32a-c, although each hash value is generated with a single processor number 30. Because each web site associates computer system 10 with a different hash value, information about a user of system 10 may not be correlated between databases that are maintained by different web sites.

To ensure that this safeguard is not circumvented by web sites 36a-c agreeing to use the same key, it may be desirable to require that each key correspond to an address or universal resource locator (URL) for each web site 36a-c. An URL based key may be reliably tied to a particular web site by making the instruction for accessing the hash value a ring 0 instruction. In response to a web site request for that hash value, the operating system can call a driver that has ring 0 privileges. The driver then causes the processor to validate the key, e.g., by checking it against the web site's URL -- which may be retrieved from the browser. If the URL matches the key, then the processor executes instructions for hashing that key with the processor number and returns the resulting hash value to the web site. If the URL does not match the key, the web site's request is rejected.

Although making hash value retrieval a ring 0 operation ensures privacy for the user, a content provider may not be comfortable relying on such an operation to ensure that delivered encrypted content, and an accompanying decryption program, runs on authorized systems only. Because inter-privilege level calls may be intercepted by rogue software, a content provider may not wish to depend on a driver (ring 0) call for this function. Content providers may instead want the decryption program to be able to invoke a ring 3 instruction to verify the identity of the computer system that executes the program.

Accordingly, there is a need for a method and apparatus that enables an application's execution to be bound to authorized platforms, while still preserving user privacy. There is a need for such a method and apparatus that enables a decryption program to detect whether a computer system is authorized to execute that program -- to ensure that delivered content is not copied for use by an unauthorized platform. There is a need for such a method and apparatus that enables such a program to periodically verify the identity of the platform upon which it is executed. The present invention provides such a method and apparatus.

SUMMARY OF THE INVENTION

A method and apparatus for enabling hardware platform identification while ensuring privacy protection is described. The apparatus comprises a computer-readable medium that stores computer-executable instructions. Those instructions, when executed by a microprocessor, cause an expected hash value, which is derived from a key and a first identifier for a computer system, to be compared with a hash value, which is derived from the key and a second identifier for a computer system. A microprocessor for executing those instructions may comprise an identifier that identifies the microprocessor, and embedded instructions for comparing a hash value, derived from the identifier and a key, to an expected hash value.

That microprocessor, and the computer-executable instructions, may be used in a method for confirming the identity of a computer system. Such a method may comprise receiving a request from an application (e.g., a decryption program) to confirm the identity of a computer system. That request may be accompanied by a key (e.g., a bit string corresponding to an URL for a web site) and an expected hash value derived from that key and a first identifier for a computer system. After a second identifier -- for the computer system that executes the application -- is retrieved, a hash value is generated, which is derived from the second identifier and the key. That hash value is then compared with the expected hash value. The result of that comparison may then be forwarded to the application.

The method and apparatus of the present invention enables a decryption program (or other application) to periodically verify the identity of a computer system during the program's execution to ensure that the system is authorized to execute that program. That identity check may be performed without having to expose a platform identifier (or hash of that identifier) to the program. This capability is thus provided without having to enable other applications to access a platform identifier, which could compromise user privacy.

BRIEF DESCRIPTION OF THE DRAWINGS

Figure 1 is a block diagram of a network connecting a computer system to a number of web sites.

Figure 2 is a block diagram illustrating the hash value comparison operation of the present invention.

Figure 3 is a block diagram of a microprocessor that may be used to perform the comparison operation illustrated in figure 2.

Figure 4 is a flow chart illustrating an embodiment of the method of the present invention.

Figure 5 is a flow chart illustrating another embodiment of the method of the present invention.

DETAILED DESCRIPTION OF THE PRESENT INVENTION

A method and apparatus is described for comparing an expected hash value to a hash value derived from a computer system identifier and a key. In the following description, numerous specific details are set forth to provide a thorough understanding of the present invention. However, it will be apparent to those skilled in the art that the invention may be practiced in many ways other than those expressly described here. The invention is thus not limited by the specific details disclosed below.

The method and apparatus of the present invention enable an application (e.g., a decryption program) to confirm the identity of a computer system. This enables an application (e.g., a decryption program for decrypting encrypted video and/or audio containing content) to perform periodic checks on the identity of a platform executing that application. This capability enables such an application to determine whether a program has been copied from an authorized system to an unauthorized system. In this respect, the method and apparatus of the present invention enable content that has been delivered to a computer system to be bound to that system.

To confirm the identity of a computer system, a microprocessor (a.k.a. processor) executes instructions for comparing an expected hash value, which may be derived from a key and a first identifier for a computer system, to a hash value derived from that key and a second identifier for a computer system. If the expected hash value matches the generated hash value, the microprocessor returns a “true” output. If the hash values do not match, a “false” output is returned.

In the context of this application, the phrase “computer system” may generally refer to a processor-based system. Such a system may include (but is not limited to) a server, a desktop computer, a mobile computer (a laptop or notebook computer, for example), a graphics system, a set-top box, a personal digital assistant, or a variety of hand held devices able to provide some type of computing function. The term “processor” may refer to, as examples, at least one central processing unit (CPU), microcontroller, X86 instruction based microprocessor (e.g., a microprocessor available from Intel Corporation under the Pentium® or Itanium® trade names, or a compatible microprocessor), Advanced RISC Machine (ARM) microprocessor or RISC processor. These examples are not intended to be limiting. Rather, other types of computer systems and other types of processors may be used in some embodiments of the invention. To generate the hash values referenced herein, many different hash functions may be used. For example, in some embodiments, a secure hash algorithm (SHA) may be used.

As shown in figure 2, the hash value comparison function of the present invention may be accomplished as follows. In the context of binding an application to a particular platform, key 201 and expected hash value 202 are fed into microprocessor 203. Key 201 may comprise a unique bit string that corresponds to a web site address, or URL, for a web site that delivers content. Microprocessor 203 generates hash value 204 from key 201 and identifier 205. Microprocessor 203 then executes instructions that cause expected hash value 202 to be compared with generated hash value 204, outputting true/false result 206. If the hash values match, result 206 is true. If they do not match, result 206 is false.

Microprocessor 203 is shown in more detail in figure 3. Microprocessor 203 includes embedded instructions that take the form of microcode, which are stored in microcode ROM 301. Other functional blocks contained within microprocessor 203 execute these microcoded instructions in response to appropriate commands, as is well known to those skilled in the art. In this embodiment of the present invention, microcode ROM 301 includes microcode routines 302 and 303. When executed, microcode routine 302 generates a hash value that is derived from processor number 304 (also stored in microprocessor 203, and which in this embodiment fills the role of identifier 205) and a key. Microcode routine 303, when executed, compares that generated hash value with an expected hash value, then returns the result of that comparison.

A preferred method of the present invention, as applied to an application (e.g., a decryption program for decrypting encrypted content) that is capable of verifying a computer system's identify, is illustrated by the flow chart shown in figure 4. In that method, an application wants to confirm the identity of a computer system. To do so, that application invokes a "compare" instruction that is accompanied by two data values, i.e., an expected hash value and a key (step 400). The expected hash value may be derived from a processor number stored on a computer system that is authorized to run the application and a bit string corresponding to an URL for a web site that delivered that application. The outcome of the "compare" instruction will determine whether the computer system that currently executes the application is identical to the computer system that is authorized to do so, e.g., the computer system to which encrypted content, and an accompanying decryption program, was initially delivered.

The computer system's microprocessor receives the request from the application to confirm the identity of the system. The microprocessor also receives the expected hash value and the key. The microprocessor then generates a hash value from the key and the processor number stored in the microprocessor (step 410). The microprocessor may perform that hashing operation by executing an appropriate microcode routine.

After the hash value has been generated, the microprocessor compares that value with the expected hash value (step 420), then returns a true/false response based on that comparison (step 430). If the hash values match, a true response is returned – indicating that the computer system currently executing the application is identical to the computer system that is authorized to execute the application (e.g., the computer system to which the application was initially delivered). If the hash values do not match, a false response is returned, notifying the application (e.g., decryption program) that the computer systems are not identical. In response to such a false response, the application can discontinue its execution.

The method and apparatus of the present invention enables an application to query a computer system's hardware to determine whether that system matches the computer system that is authorized to execute the application. Because the microprocessor returns a true/false answer in response to that request, neither the computer system's processor number, nor a hash value derived from it, is exposed when the application performs this identity check. As a consequence, such a system identifier need not be exposed to other applications, and user privacy is preserved.

The method and apparatus of the present invention thus provides a hardware feature that preserves consumer privacy protection while enabling an application to reliably verify the identity of a computer system. In a system that employs the present invention, an application that already knows the hash value corresponding to a particular computer system, i.e., the expected hash value referenced above, can validate that it has not been copied over to an unauthorized system. Such an application can be bound to a platform (e.g., one receiving the authorized delivery of encrypted content and an accompanying decryption program) by simply having the computer system's hardware compare an expected hash value with the hash value derived from a key and the system's processor number.

Figure 5 provides a flow chart that illustrates how the method and apparatus of the present invention may be used to tie content, delivered from a web site, to a platform. A computer system requests the delivery of content from a web site (step 500). In response, the web site requests the computer system to return a hash value – e.g., a hash value derived from the computer system's processor number and a string that corresponds to the web site's URL (step 510). The computer system returns that hash value to the web site (step 520). The web site then sends encrypted content, and an accompanying decryption program, to the computer system (step 530). That decryption program may be embodied in a tamper resistant form – as described in U.S. Patent 5,892,899, issued April 6, 1999 and assigned to this application's assignee.

In this embodiment of the present invention, the decryption program includes the hash value that had been returned by the computer system (i.e., the "expected hash value"), and code (also embodied in a tamper resistant form) that performs periodic platform identity checks, as that program is executed. In a preferred embodiment, that code periodically invokes an instruction that causes the expected hash value to be compared with a hash value derived from the key (e.g., the string corresponding to the URL for the web site that delivered the encrypted content) and the processor number for the platform that currently executes the program (step 540). If the hash values match, the platform continues to execute the program (step 550). If the hash values do not match, suggesting that the program was improperly copied from the system that initially received it to another system, the program can discontinue execution (step 560).

By including in the decryption program, code that periodically invokes the hash value comparison function described above, execution of that program can be tied to the platform that initially received the program and the accompanying encrypted content. By embodying that code in tamper resistant form, a user should not be able to determine when such periodic checks occur, making it very difficult for a user to copy the program over to another system. In addition, if a ring 3 instruction is used to perform such periodic checks, no system call is required, which, unlike a ring 0 instruction, ensures that rogue software cannot intercept an inter-privilege call.

Although the foregoing description has specified a preferred embodiment of a method and apparatus for identifying a computer system, while preserving user privacy, those skilled in the art will appreciate that many modifications and substitutions may be made. For example, the processor number may be replaced by another identifier that identifies a computer system. A key other than a string that corresponds to an URL may be used. Applications other than applications delivered from web sites may request computer system identification. For example, such requests may be delivered to a computer system via a local area network (LAN). In addition, applications to be executed on licensed platforms only may use this method and apparatus to bind execution to licensed systems. Although presented in the context of a download from a web site, the encrypted content and the decryption program may be delivered to the platform in other ways, e.g., via delivery of a self-contained storage device (e.g., floppy disc, CD-ROM, DVD-ROM, etc. . .). Similarly, although presented in the context of binding content to a specific platform, the method and apparatus of the present invention may be used to authenticate computer systems for other purposes. Accordingly, it is intended that these and all other modifications, alterations, substitutions and additions be considered to fall within the spirit and scope of the invention as defined by the appended claims.

What is claimed is:

1. A microprocessor comprising:

an identifier that identifies the microprocessor; and

embedded instructions for comparing a hash value, derived from the identifier and a key, to an expected hash value.

2. The microprocessor of claim 1 further comprising embedded instructions for producing a hash value that is a function of the identifier and a key.

3. The microprocessor of claim 2 wherein the identifier comprises a processor number.

4. The microprocessor of claim 3 wherein the embedded instructions comprise microcode.

5. The microprocessor of claim 4 wherein the key corresponds to an address for a web site.

6. The microprocessor of claim 5 wherein the expected hash value is derived from a key that corresponds to an address for a web site and a processor number.

7. A computer-readable medium having computer-executable instructions stored therein that, when executed by a microprocessor, cause an expected hash value, which is derived from a key and a first identifier for a computer system, to be compared with a hash value, which is derived from the key and a second identifier for a computer system.

8. The computer-readable medium of claim 7 further comprising computer-executable instructions stored therein that, when executed by a microprocessor, cause the result of that comparison to be communicated to an application.

9. The computer-readable medium of claim 8 wherein the application comprises a decryption program.

10. A server comprising:

a computer-readable medium having computer-executable instructions stored therein that, when executed by a microprocessor, cause an expected hash value, which is derived from a key corresponding to a web site and a first identifier for a computer system, to be compared with a hash value, which is derived from the key and a second identifier for a computer system.

11. The server of claim 10 wherein the computer-executable instructions comprise a decryption program and wherein the computer-readable medium further comprises computer-executable instructions stored therein that, when executed by a microprocessor, cause the result of that comparison to be communicated to the decryption program.

12. A method for confirming the identity of a computer system comprising:

transmitting a request from an application to a computer system to confirm the identity of the computer system, the request accompanied by a key and an expected hash value derived from that key and a first identifier for a computer system;

retrieving a second identifier that identifies the computer system;

generating a hash value derived from the second identifier and the key; and

comparing that hash value with the expected hash value.

13. The method of claim 12 wherein the application comprises a decryption program and wherein the method further comprises:

storing the result of the hash value comparison; and

forwarding that result to the decryption program.

14. The method of claim 13 wherein the first and second identifiers are each processor numbers.

15. The method of claim 14 wherein the key comprises a unique bit string that corresponds to a web site address.

16. The method of claim 13 further comprising returning a true response if the first and second processor numbers are identical, and returning a false response if the first and second processor numbers are not identical.

17. A method for binding an application to a computer system comprising:

periodically checking the identity of a computer system as it executes an application to ensure that the computer system is authorized to execute the application, such periodic checks performed by:

delivering to a microprocessor a key and an expected hash value, derived from the key and a first processor number for a computer system; and

instructing the microprocessor to compare that expected hash value to a hash value derived from that key and the processor number for the computer system that is executing the program, then to return to the application the result of that comparison.

18. The method of claim 17 wherein the application comprises a decryption program.

19. The method of claim 18 wherein the instructions for requesting the hash value comparison are embodied in tamper resistant software.

20. A computer-readable medium having computer-executable instructions stored therein that, when executed by a microprocessor, cause the identity of a computer system to be periodically checked as it executes an application to ensure that the computer system is authorized to execute the application, such periodic checks performed by:

delivering to a microprocessor a key and an expected hash value, derived from the key and a first processor number for a computer system; and

instructing the microprocessor to compare that expected hash value to a hash value derived from that key and the processor number for the computer system that is executing the program, then to return to the application the result of that comparison.

21. A method for binding the execution of encrypted content, and an accompanying decryption program, to a platform comprising:

transmitting to a computer system encrypted content, and an accompanying decryption program, the decryption program comprising a hash value and instructions for performing periodic checks on the identity of any computer system that executes the decryption program, as that program is executed; and

performing those periodic identity checks by comparing the hash value delivered by the decryption program with a second hash value derived at least in part from an identifier for the computer system that executes the program.

22. The method of claim 21 wherein the hash value is derived from the processor number for the computer system that received from a web site the encrypted content and accompanying decryption program, and a bit string that corresponds to an URL for that web site.

23. The method of claim 22 wherein the computer system delivered the hash value to the web site before the web site delivered the encrypted content, and accompanying decryption program, to the computer system.

24. The method of claim 23 wherein the decryption program, including the instructions for performing the periodic identity checks, are embodied in tamper resistant software.

ABSTRACT

A method and apparatus for enabling hardware platform identification while ensuring privacy protection. The apparatus comprises a computer-readable medium that stores computer-executable instructions. Those instructions, when executed by a microprocessor, cause an expected hash value, which is derived from a key and a first identifier for a computer system, to be compared with a hash value, which is derived from the key and a second identifier for a computer system. A microprocessor for executing those instructions may comprise an identifier that identifies the microprocessor, and embedded instructions for comparing a hash value, derived from the identifier and a key, to an expected hash value.

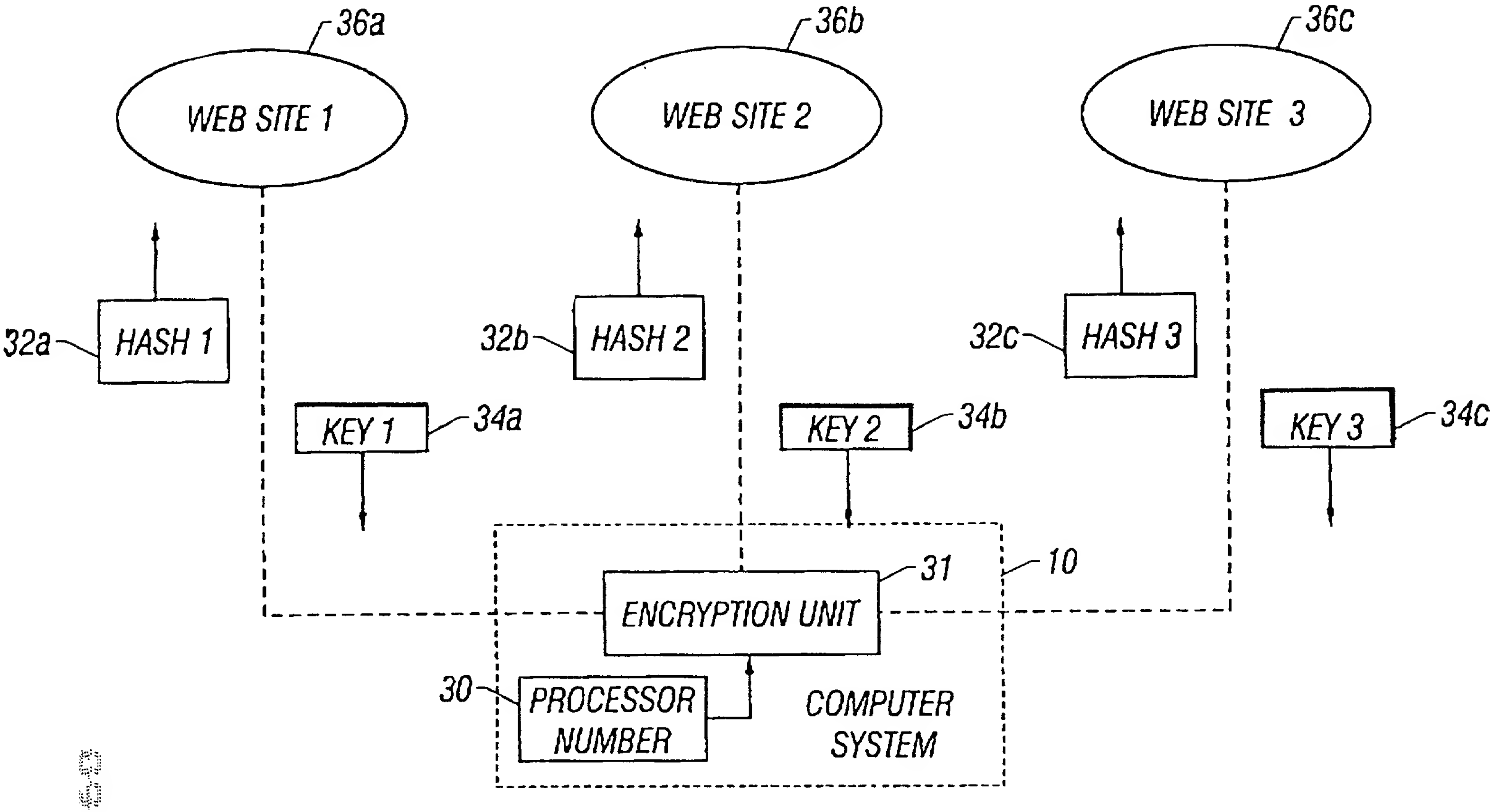

FIG. 1

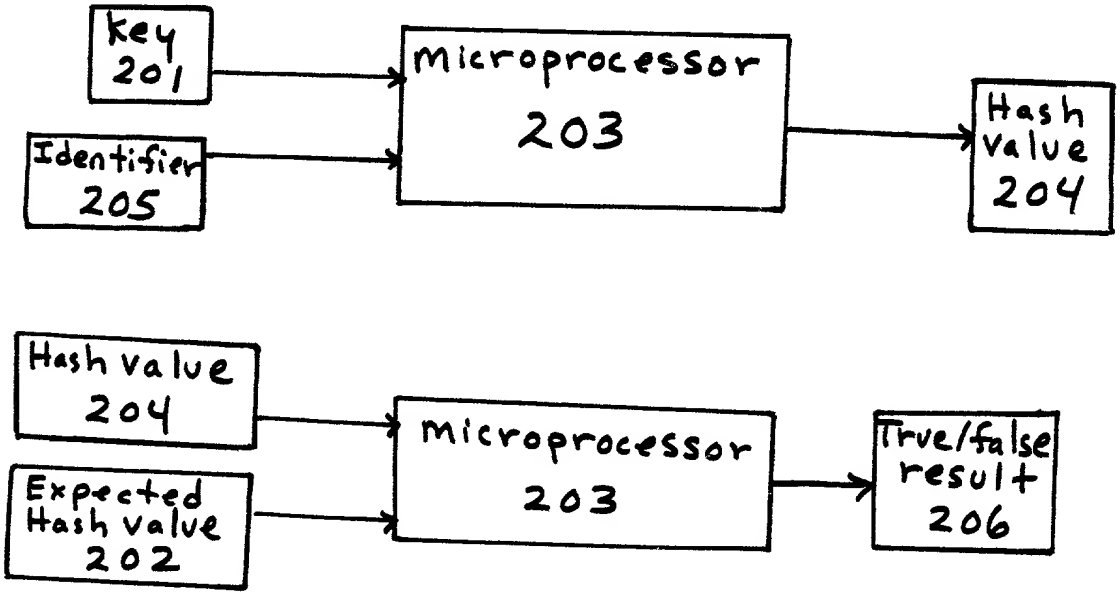

Figure 2

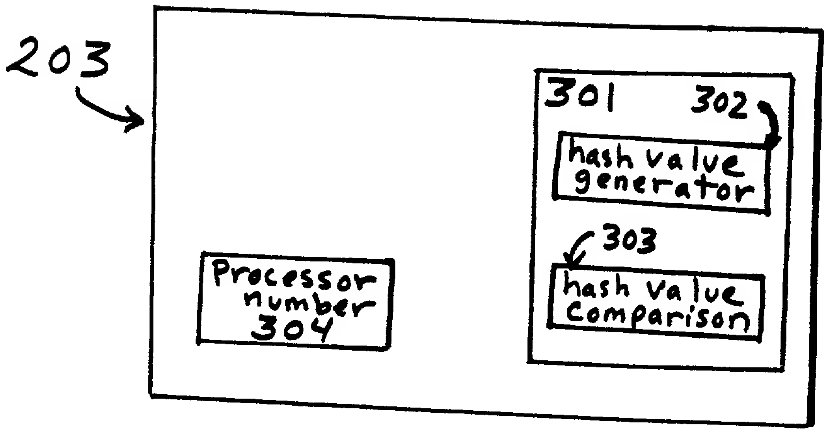

Figure 3

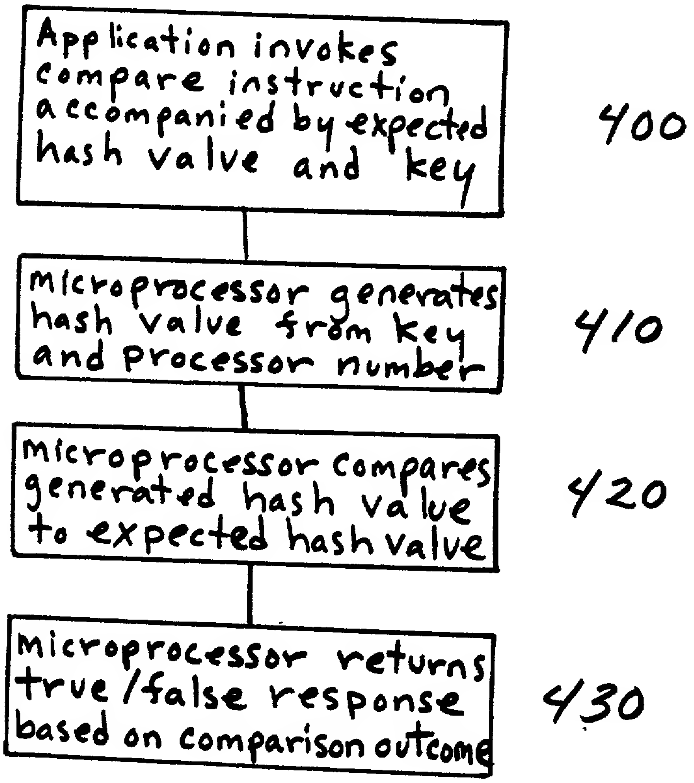
Application invokes compare instruction accompanied by expected hash value and key
400
microprocessor generates hash value from key and processor number
410
microprocessor compares generated hash value to expected hash value
420
Microprocessor returns true/false response based on comparison outcome
430

Figure 4

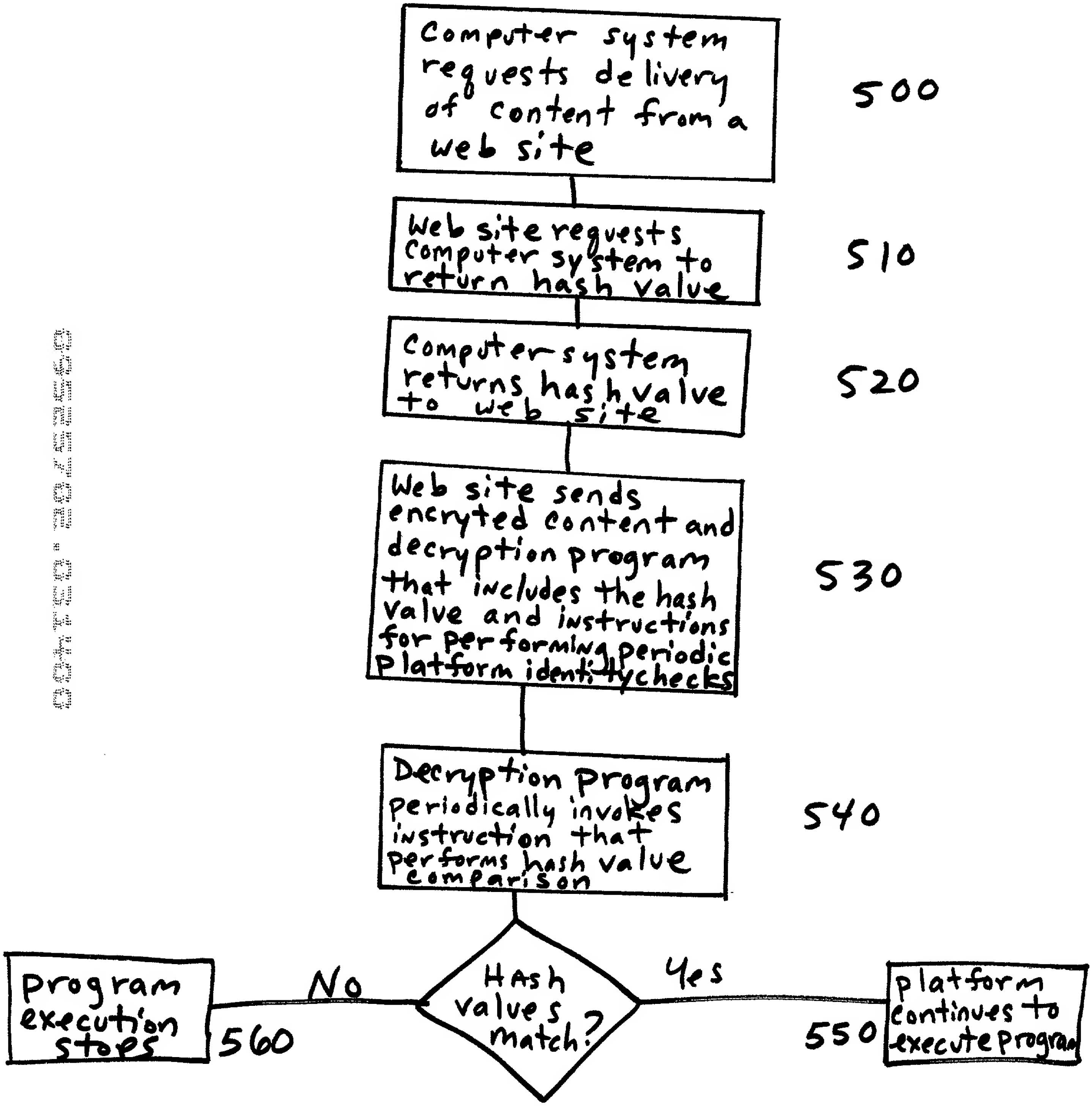
Computer system requests delivery of content from a web site
500
Web site requests Computer system to return hash value
510
Computer system returns hash value to web site
520
Web site sends encryted content and decryption program that includes the hash value and instructions for performing periodic platform identity checks
530
Decryption program periodically invokes instruction that performs hash value comparison
540
Hash values match?
No
Yes
program execution stops
560
platform continues to execute program
550

Figure 5

Attorney's Docket No.: 42390.P7440 PATENT

DECLARATION AND POWER OF ATTORNEY

As a below named inventor, I hereby declare that:

My residence, post office address and citizenship are as stated below next to my name.

I believe I am an original, first, and joint inventor of the subject matter which is claimed and for which a patent is sought on the invention entitled

METHOD AND APPARATUS FOR HARDWARE
PLATFORM IDENTIFICATION WITH PRIVACY PROTECTION

the specification of which

x is attached hereto.
_____ was filed on _______________ as
United States Application Number ______________
or PCT International Application Number ______
and was amended on ________________________
(if applicable)

I hereby state that I have reviewed and understand the contents of the above-identified specification, including the claim(s), as amended by any amendment referred to above. I do not know and do not believe that the claimed invention was ever known or used in the United States of America before my invention thereof, or patented or described in any printed publication in any country before my invention thereof or more than one year prior to this application, that the same was not in public use or on sale in the United States of America more than one year prior to this application, and that the invention has not been patented or made the subject of an inventor's certificate issued before the date of this application in any country foreign to the United States of America on an application filed by me or my legal representatives or assigns more than twelve months (for a utility patent application) or six months (for a design patent application) prior to this application.

I acknowledge the duty to disclose all information known to me to be material to patentability as defined in Title 37, Code of Federal Regulations, Section 1.56.

I hereby claim foreign priority benefits under Title 35, United States Code, Section 119(a)-(d), of any foreign applications for patent or inventor's certificate listed below and have also identified below any foreign application for patent or inventor's certificate having a filing date before that of the application on which priority is claimed:

Priority
Claimed

(Number) (Country) (Day/Month/Year Filed) Yes No

(Number) (Country) (Day/Month/Year Filed) Yes No

(Number) (Country) (Day/Month/Year Filed) Yes No

I hereby claim the benefit under title 35, United States Code, Section 119(e) of any United States provisional application(s) listed below

(Application Number) Filing Date

(Application Number) Filing Date

I hereby claim the benefit under Title 35, United States Code, Section 120 of any United States application(s) listed below and, insofar as the subject matter of each of the claims of this application is not disclosed in the prior United States application in the manner provided by the first paragraph of Title 35, United States Code, Section 112, I acknowledge the duty to disclose all information known to me to be material to patentability as defined in Title 37, Code of Federal Regulations, Section 1.56 which became available between the filing date of the prior application and the national or PCT international filing date of this application:

(Application Number) Filing Date (Status—patented, pending, abandoned)

I hereby appoint Aloysius T. C. AuYeung, Reg. No. 3S,432; William Thomas Babbitt, Reg. No. 39,591; Kent D. Baker, Reg. No. 38,822; Jordan Michael Becker, Reg. No. 39,602; Bradley J. Bereznak, Reg. No. 33,474; Michael A. Bernadicou, Reg. No. 35,934; Roger W. Bravely, Jr., Reg. No. 25,831; Gregory D. Caldwell, Reg. No. 39 926; Kent M. Chen, Reg. No. 39,630; Lawrence M. Cho, Reg. No. 39,942; Thomas M. Coester, Reg. No P39,637; Roland B. Cortes, Reg. No. 39,152; William Donald Davis, Reg. No. 38,428; [Daniel M De Vos, Reg. No. 37,813; Karen L. Feisthamel, Reg. No. 40,264; David R. Halvorson, Reg. No. 33,395; Brian Don Hickman. Reg. No. 35,894; Eric Ho, Reg. No. P39,711; George W Hoover II, Reg. No. 32,992; Eric S. Hyman, Reg. No. 30,139, Jeffrey D. Jacobs, Reg. No. 40,029; Dag H. Johansen, Reg. No. 36,172; Stephen L. King, Reg. No. 19,180; Dolly M. Lee, Reg. No. 39,742; Michael J.

Marie, Reg. No. 36,591; Kimberley G. Nobles, Reg. No. 38,255; Ronald W. Reagin, Reg. No. 20,340; James H Salter, Reg. No. 35,668, William W. Schaal, Reg. No. 39,018; James C. Scheller, Reg. No. 3X,195; Maria McCormack Sobrino, Reg. No. 31,639; Stanley W. Sokoloff, Reg. No. 2S,128; Allan T. Sponseller, Reg. No. 38,318; Steven R. Sponseller, Reg. No. 39,384; David R. Stevens, Reg. No. 3B,626; Edwin H. Taylor, Reg. No. 25,129; Lester J. Vincent, Reg. No. 31,460; John Patrick Alard, Reg. No. 40,216; Ben J. Yorks, Reg. No. 33,609; and Norman Zafman, Reg. No. 26,250; my attorneys; and Gary B. Goates, Reg. No. 35,159; Michael Anthony DeSanctis, Reg. No. 39,957; Charles E. Shemwell, Reg. No. 40,171; Edwin A. Sloane, Reg. No. 34,728; and Judith A. Szepesi, Reg. No. 39,393; my patent agents, of BLAKELY, SOKOLOFF, TAYLOR & ZAFMAN, with offices located at 12400 Wilshire Boulevard, 7th Floor, Los Angeles, California 9002E, telephone (310) 207-3800, and Joseph R. Bond, Reg. No. 36,458; Richard C. Calderwood, Reg. No. 35,468, Mark Seeley, Reg. No. 32,299; Leo V. Novakoski, Reg. No. 37,198; Naomi Obinata, Reg. No. 39,320; Thomas C. Reynolds, Reg. No. 32,488; and Raymond J. Werner, Reg. No. 34,752 of INTEL CORPORATION with full power of substitution and revocation, to prosecute this application and to transact all business in the Patent and Trademark Office connected herewith.

Send correspondence to Mark Seeley, c/o BLAKELY, SOKOLOFF, TAYLOR & ZAFMAN, 12400 Wilshire Boulevard, 7th Floor, Los Angeles, California 90025 and direct telephone calls to Mark Seeley, (408) 765-7382.

I hereby declare that all statements made herein of my own knowledge are true and that all statements made on information and belief are believed to be true; and further that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under Section 1001 of Title 18 of the United States Code and that such willful false statements may jeopardize the validity of the application or any patent issued thereon.

Full Name of Sole/First Inventor Millind Mittal

Inventor's Signature ______________ Date 3/1/2000

Residence 800 E. Charleston Rd. #29, Palo Alto, CA 94303 Citizenship US
(City, State) (Country)

Post Office Address Same as above

Full Name of Second/Joint Inventor James Mi

Inventor's Signature ________________________ Date ____________________________

Residence 1361 Fisherhawk Way, Sunnyvale, CA 94087 Citizenship China
(City, State) (Country)

Post Office Address Same as above

Attorney's Docket No.: 42390.P7440 PATENT

DECLARATION AND POWER OF ATTORNEY

As a below named inventor, I hereby declare that:

My residence, post office address and citizenship are as stated below next to my name.

I believe I am an original, first, and joint inventor of the subject matter which is claimed and for which a patent is sought on the invention entitled

METHOD AND APPARATUS FOR HARDWARE
PLATFORM IDENTIFICATION WITH PRIVACY PROTECTION

the specification of which

x is attached hereto.
_____ was filed on _______________ as
United States Application Number _____________
or PCT International Application Number ______
and was amended on _________________________
(if applicable)

I hereby state that I have reviewed and understand the contents of the above-identified specification, including the claim(s), as amended by any amendment referred to above. I do not know and do not believe that the claimed invention was ever known or used in the United States of America before my invention thereof, or patented or described in any printed publication in any country before my invention thereof or more than one year prior to this application, that the same was not in public use or on sale in the United States of America more than one year prior to this application, and that the invention has not been patented or made the subject of an inventor's certificate issued before the date of this application in any country foreign to the United States of America on an application filed by me or my legal representatives or assigns more than twelve months (for a utility patent application) or six months (for a design patent application) prior to this application.

I acknowledge the duty to disclose all information known to me to be material to patentability as defined in Title 37, Code of Federal Regulations, Section 1.56.

I hereby claim foreign priority benefits under Title 35, United States Code, Section 119(a)-(d), of any foreign applications for patent or inventor's certificate listed below and have also identified below any foreign application for patent or inventor's certificate having a filing date before that of the application on which priority is claimed:

Priority
Claimed

(Number) (Country) (Day/Month/Year Filed) Yes No

(Number) (Country) (Day/Month/Year Filed) Yes No

(Number) (Country) (Day/Month/Year Filed) Yes No

I hereby claim the benefit under title 35, United States Code, Section 119(e) of any United States provisional application(s) listed below

(Application Number) Filing Date

(Application Number) Filing Date

I hereby claim the benefit under Title 35, United States Code, Section 120 of any United States application(s) listed below and, insofar as the subject matter of each of the claims of this application is not disclosed in the prior United States application in the manner provided by the first paragraph of Title 35, United States Code, Section 112, I acknowledge the duty to disclose all information known to me to be material to patentability as defined in Title 37, Code of Federal Regulations, Section 1.56 which became available between the filing date of the prior application and the national or PCT international filing date of this application:

(Application Number) Filing Date (Status—patented, pending, abandoned)

I hereby appoint Aloysius T. C. AuYeung, Reg. No. 3S,432; William Thomas Babbitt, Reg. No. 39,591; Kent D. Baker, Reg. No. 38,822; Jordan Michael Becker, Reg. No. 39,602; Bradley J. Bereznak, Reg. No. 33,474; Michael A. Bernadicou, Reg. No. 35,934; Roger W. Bravely, Jr., Reg. No. 25,831; Gregory D. Caldwell, Reg. No. 39 926; Kent M. Chen, Reg. No. 39,630; Lawrence M. Cho, Reg. No. 39,942; Thomas M. Coester, Reg. No P39,637; Roland B. Cortes, Reg. No. 39,152; William Donald Davis, Reg. No. 38,428; [Daniel M De Vos, Reg. No. 37,813; Karen L. Feistharnel, Reg. No. 40,264; David R. Halvorson, Reg. No. 33,395; Brian Don Hickman. Reg. No. 35,894; Eric Ho, Reg. No. P39,711; George W Hoover II, Reg. No. 32,992; Eric S. Hyman, Reg. No. 30,139, Jeffrey D. Jacobs, Reg. No. 40,029; Dag H. Johansen, Reg. No. 36,172; Stephen L. King, Reg. No. 19,180; Dolly M. Lee, Reg. No. 39,742; Michael J.

Marie, Reg. No. 36,591; Kimberley G. Nobles, Reg. No. 38,255; Ronald W. Reagin, Reg. No. 20,340; James H Salter, Reg. No. 35,668, William W. Schaal, Reg. No. 39,018; James C. Scheller, Reg. No. 3X,195; Maria McCormack Sobrino, Reg. No. 31,639; Stanley W. Sokoloff, Reg. No. 2S,128; Allan T. Sponseller, Reg. No. 38,318; Steven R. Sponseller, Reg. No. 39,384; David R. Stevens, Reg. No. 3B,626; Edwin H. Taylor, Reg. No. 25,129; Lester J. Vincent, Reg. No. 31,460; John Patrick Alard, Reg. No. 40,216; Ben J. Yorks, Reg. No. 33,609; and Norman Zafman, Reg. No. 26,250; my attorneys; and Gary B. Goates, Reg. No. 35,159; Michael Anthony DeSanctis, Reg. No. 39,957; Charles E. Shemwell, Reg. No. 40,171; Edwin A. Sloane, Reg. No. 34,728; and Judith A. Szepesi, Reg. No. 39,393; my patent agents, of BLAKELY, SOKOLOFF, TAYLOR & ZAFMAN, with offices located at 12400 Wilshire Boulevard, 7th Floor, Los Angeles, California 9002E, telephone (310) 207-3800, and Joseph R. Bond, Reg. No. 36,458; Richard C. Calderwood, Reg. No. 35,468, Mark Seeley, Reg. No. 32,299; Leo V. Novakoski, Reg. No. 37,198; Naomi Obinata, Reg. No. 39,320; Thomas C. Reynolds, Reg. No. 32,488; and Raymond J. Werner, Reg. No. 34,752 of INTEL CORPORATION with full power of substitution and revocation, to prosecute this application and to transact all business in the Patent and Trademark Office connected herewith.

Send correspondence to Mark Seeley, c/o BLAKELY, SOKOLOFF, TAYLOR & ZAFMAN, 12400 Wilshire Boulevard, 7th Floor, Los Angeles, California 90025 and direct telephone calls to Mark Seeley, (408) 765-7382.

I hereby declare that all statements made herein of my own knowledge are true and that all statements made on information and belief are believed to be true; and further that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under Section 1001 of Title 18 of the United States Code and that such willful false statements may jeopardize the validity of the application or any patent issued thereon.

Full Name of Sole/First Inventor Millind Mittal

Inventor's Signature ______________________ Date __________________________

Residence 800 E. Charleston Rd. #29, Palo Alto, CA 94303 Citizenship US
(City, State) (Country)

Post Office Address Same as above

Full Name of Second/Joint Inventor James Mi

Inventor's Signature ______________ Date 3/4/2000

Residence 1361 Fisherhawk Drive, Sunnyvale, CA 94087 Citizenship China
(City, State) (Country)

Post Office Address Same as above